Journal of Information Security, 2014, 5, 166-177
Published Online October 2014 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2014.54016

A Conceptual Framework for Threat Assessment Based on Organization's Information Security Policy

Joseph Elias Mbowe[1], Irina Zlotnikova[1], Simon S. Msanjila[2], George S. Oreku[3]

[1]School of Computational Science and Communication Engineering, The Nelson Mandela African Institution of Science and Technology, Arusha, Tanzania
[2]Faculty of Science and Technology, Mzumbe University, Morogoro, Tanzania
[3]Faculty of Economics, North West University, Vanderbijlpark, South Africa
Email: mbowej@nm-aist.ac.tz, irina.zlotnikova@nm-aist.ac.tz, simon.msanjila@mzumbe.ac.tz, george.oreku@tirdo.ac.tz

Received 12 July 2014; revised 10 August 2014; accepted 5 September 2014

Abstract

The security breaches of sensitive information have remained difficult to solve due to increased malware programs and unauthorized access to data stored in critical assets. As risk appetite differ from one organization to another, it prompts the threat analysis tools be integrated with organization's information security policy so as to ensure security controls at local settings. However, it has been noted that the current tools for threat assessment processes have not encompassed information security policy for effective security management (*i.e.* confidentiality, integrity and availability) based on organization's risk appetite and culture. The information security policy serves as a tool to provide guidance on how to manage and secure all business operations including critical assets, infrastructure and people in the organization. This guidance (e.g. usage and controls) facilitates the provisions for threat assessment and compliance based on local context. The lack of effective threat assessment frameworks at local context have promoted the exposure of critical assets such as database servers, mails servers, web servers and user smart-devices at the hand of attackers and thus increase risks and probability to compromise the assets. In this paper we have proposed a conceptual framework for security threat assessment based on organization's information security policy. Furthermore, the study proposed the policy automation canvas for provision of a methodology to alert the security managers what possible threats found in their organizations for quick security mitigation without depending on security expertise.

Keywords

Critical Asset, Information Security, Information Security Policy, Threat Analysis, Threat

How to cite this paper: Mbowe, J.E., Zlotnikova, I., Msanjila, S.S. and Oreku, G.S. (2014) A Conceptual Framework for Threat Assessment Based on Organization's Information Security Policy. *Journal of Information Security*, **5**, 166-177. http://dx.doi.org/10.4236/jis.2014.54016

Assessment, Security Threat Visualization

1. Introduction

As technology advances, the data or information has become the valuable asset in many organizations and thus it is so challenging to protect them from the hands of attackers [1]-[5]. The recent report has shown that, the security breaches of information stored into ICT assets (e.g. systems which accept, process and store data) have remained difficult to solve (see **Figure 1**) the percent of major threats actions and associated potential assets been exploited [6]. As shown in **Figure 1**, apart from physical theft and stolen cards, the problem of unauthorized access to data by using advanced technologies (e.g. hacking and malware programs such as phishing, privilege abuse, back doors, key loggers and data exporters) have become a big challenge in the management of information security systems.

While these hacking and malware technologies' overwhelming globally, Tanzania has not been left behind in using the mobile and internet technologies and therefore we expect the country to suffer from cybercrime as time goes. The current trend has shown that there exist substantive security breaches in Tanzania (see **Figure 2**) computer related cases in Tanzania. Despite the existing cybercrime, no cyber law exists to protect the information stored into computer systems. The existing Electronic and Postal Communications Act, 2007 do not adequately address cyber issues to safeguards at national-wide the IT resources and guarantee the security services such as confidentiality, integrity and availability.

Due to persistent of cyber crime globally and computer related cases in Tanzania, we have investigated the extent of security problem in public organizations and thus propose a framework for security threats assessment based on organization's information security policy. Various tools available for this purpose of security threat

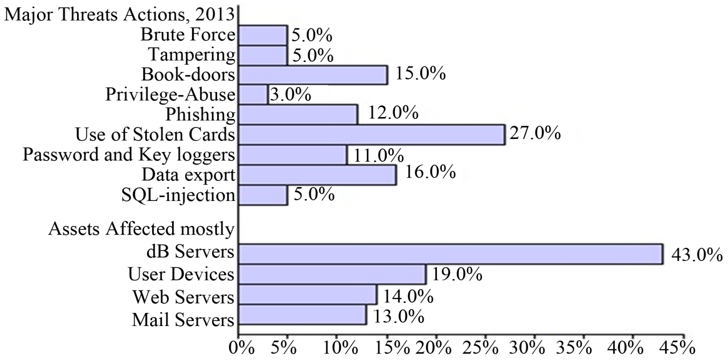


Figure 1. Major threats versus assets affected as reported by data breach invenstigation report (DBIR, 2014).

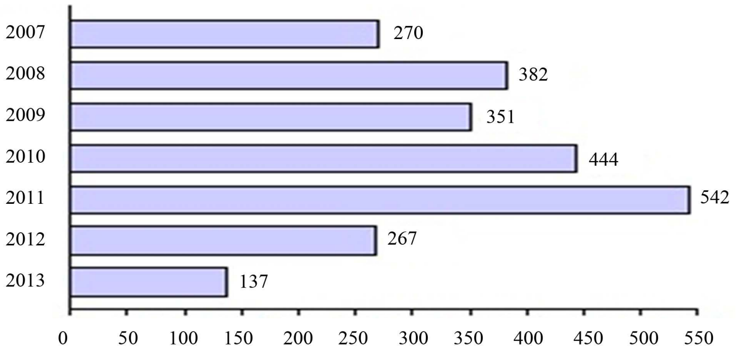


Figure 2. Computer related cases in Tanzania as reported to the Cyber Crime Unit under Ministry of Home Affairs.

assessment such as Common Criteria, OCTAVE, CORAS and CySeMoL, have not integrated the organization's information security policy into their threat assessment processes. Also, previous studies [7]-[11] have shown that these popular security analysis tools do suffer from being either ultimately complex to adapt or too limited in terms of expertise and public organization's environment. For example:

- Common Criteria [7] and OCTAVE [8] are very complex to adapt and they focused mainly on identifying risks that affect mostly the availability and integrity services which are of lesser importance compared to confidentiality (*i.e.* data privacy) in the public organizations.
- CORAS [9], Microsoft Threat Modelling Tool (TMT) [10] and CySeMoL [11] are very limited to UML notations. Despite their intuitive UML graphical presentation, these models do lack adequate approaches for UML interpretation so as to communicate their messages across organization pyramid.

In this paper, we have investigated the security problem and analyzed the cybercrime entrance doors (e.g. insecurity channels) from five public organizations, and then proposed the framework for threat assessment based on organization's security policy so that, security threats can be evaluated based on organization's risk appetite and culture. The paper is organized as follows: Section 2 discusses the objectives and research outcomes. Section 3 discusses an overview of security analysis tools. Section 4 is the methodology used for data collections. Section 5 represents the results and discussions. Section 6 introduces the conceptual framework for threat assessment based on security policy and finally Section 7 gives the conclusions and thereafter acknowledgement and references.

2. Research Objectives and Outcomes

Although much effort has been done on security threats analysis, there exist inadequate frameworks to fulfill the organization's information security policy and culture. Thus ensuring effective Information Security Management Systems (ISMS) based on local environment. As a result the assets storing data into computer systems are witnessing the severe security problem because it so challenging for the non-security experts to assess critically these security threats based on the organization's security policy and environment.

This challenge will continue to persist due to continuous innovations and discoveries of various sophisticated technologies such as hacking tools and malware programs. The localized framework for threat assessment to detect and visualize the critical security controls at local settings is necessary to ensure the knowledge support in management of information security at public organizations where confidentiality and integrity are of paramount. To achieve this goal, the following specific objectives have been identified:

- To identify information insecurity channels in public organizations in order to develop a comprehensive framework for knowledge support in management of information security systems.
- To develop a framework to enable software developers implement the threat assessment tools for visual demonstrations of information insecurity channels based on the organization's information security policy (e.g. approved guidelines and policies).

This study presents the following outcomes:

- The analyzed security maturity level and security threats of selected organizations and thus enrich the Information Security Management Systems (ISMS) in public organizations.
- The framework to enable development of an alert system to evaluate the critical security controls based on organization's security policy for effective cyber defense in an easy way without being a security expert.

3. Overview of Security Analysis Tools

The word security analysis describes the mechanisms for examining and assessing the various threats that undermine the security services. The tool used to evaluate the security is called security analysis tool. A number of security tools that apply the concept of UML (e.g. Unified Modelling Languages which define a methodology to visualize and represent a system graphically using symbols and diagram) have been developed. Some of these UML Threat assessment tools include CORAS, MS Threat Modeling Tool and CySeMoL. Also, there exist non-UML tools such as Common Criteria and OCTAVE. The overview of each tool is discussed hereunder.

3.1. Common Criteria

The ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation is a security standard that considers critical asset as Target of Evaluation (ToE) by imposing countermeasures for minimizing risks from the critical assets [7]. The model is driven by evaluation processes which practically depend on third-party to implement the quick wins to protect these assets. Also, the model requires comprehensive asset documentation (e.g. process, operations, products, associated threats and controls) as a results, it incurs high costs in terms of expertise, time and money.

3.2. OCTAVE

OCTAVE stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation. The OCTAVE performs security analysis by identifying critical information assets and their security requirements and thereafter put appropriate security controls in all organizational and/or technological vulnerabilities [8]. The methodology depends on both technology based and nontechnology based risks including people and organizational facilities [12]. This methodology demands a considerable amount of paperwork and investment in human resources and time in order to implement the process and documentation management across organization structure [13].

3.3. CORAS

This tool uses graphical representation approach as a fundamental language to communicate, document and analyses the security threat and risk scenarios [9]. It is the model-driven tool which uses threat diagrams to identify and document how vulnerabilities may be exploited by threats and thus initiate the unwanted incidents in a particular asset with associated likelihood estimates and possible consequences. The methodology involves eight steps for complete identification of threats and its appropriate mitigation as shown in **Figure 3** the eight steps of CORAS [14]. The main challenge of this methodology is how to establish all assumptions in all steps to attain the optimal results and the scope. Undergoing all eight steps requires series of seminars and workshops making this methodology complex and costly, especially in developing countries where the funds for IT projects and technical expertise are very limited or do not exist.

3.4. MS Threat Modelling Tool

This is Microsoft Threat Modelling tool which generate automatically the potential security vulnerabilities in the software development components such as; data flow, data store, process circle, multi-processes, inter-actors and system trust boundaries [10]. This tool employs STRIDE threat modeling techniques which decompose a system into relevant components, analyze each component for susceptibility to the threats, and mitigate the threats. The STRIDE activities include:

- Spoofing identity: forging authentication and authorization credentials for illegal or personal interests.
- Tempering with data: modifying to suite the personal interests.
- Repudiation: denying an action without other parties having mechanisms to prove otherwise.
- Information Disclosure: exposing information to individuals who are not supposed to have an access to it.
- Denial of Services: denying service or operation to genuine users or entity for smooth business operations.
- Elevation of privileges: gaining privileged access or resources without having the sufficient privilege rights in the entire system.

The major challenge of this framework focuses on software development components and thus become very

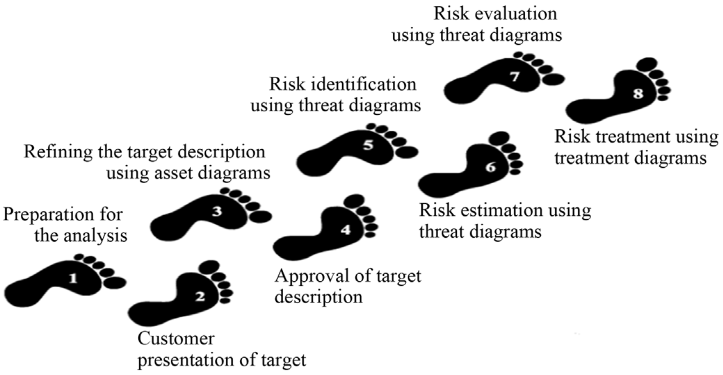

Risk evaluation using threat diagrams
Risk identification using threat diagrams
8
7
Risk treatment using treatment diagrams
Refining the target description using asset diagrams
5
6
Preparation for the analysis
3
4
Risk estimation using threat diagrams
1
2
Approval of target description
Customer presentation of target

Figure 3. The eight steps of CORA’s methodology.

useful in the early stages of software development. In this case, it is not suitable for analyzing system susceptibility to the threats after being implemented or at operational stages.

3.5. CySeMoL

The Cyber Security Modelling Language (CySeMoL) has been implemented in a software tool, the Enterprise Architecture Analysis Tool (EAAT) that enables a user-friendly interface for both modelling and analysis [11]. It has the calculation engine for estimating the cyber security at enterprise-level by describing attacks and defenses quantitatively based on Predictive, Probabilistic Architecture Modelling Framework (P^2AMF). The P^2AMF is an extension of the Object Constraint Language for probabilistic assessment and prediction of system properties. In CySeMoL, there are four types of concepts; Attacker, AttackStep, Defense and Asset as the base-objects for security threats modelling. Although the EAAT has ability to model these concepts from the scratch, the CySeMoL do not allow its users to model them manually due to complexity in defining their properties. A user is restricted to depict templates that relate attack steps and defenses to a given asset and thus limit the robustness of CySeMoL in assessing and predicting the system properties based on specific organization's environment and culture.

4. Research Methodology

In order to achieve the goal towards threat assessment based organization's local settings; we have selected five organizations to participate in the research. These public organizations named V, W, X, Y, Z to the large extent have adopted ICT to run and manage their core business services such as; raw score and grades for public examinations, registration data for births and deaths certificates, citizenship identities, data for universities selection and admissions and data for higher students' loan calculations and beneficiaries respectively.

Data were collected through observations and questionnaires. Two structured sample questionnaires were designed; one for IT staff to assess the security maturity level and insecurity channels affecting the data confidentiality and integrity as a fundamental services in public organizations and the other questionnaire for non-IT staff to assess general knowledge of information security programs and also validate the responses obtained from technical point of view. About 108 participants (e.g. 23 IT staff and 85 non IT staff) were selected to participate in the research as shown on **Table 1**.

During instruments design a Likert scale of;

- *five points*, 0—Not performed, 1—performed informally, 2—planned, 3—well defined, 4—Quantitatively controlled and 5—Continuously improving was adopted for IT staff to assess the organization maturity level and insecurity channels. For the purpose of maturity level, about 101 questions were adopted from ISO 21827 [15].
- *three points*, 0—Not Done, 1—Not Sure, 2—Sometimes 3—Yes was used for non-IT staff to assess general knowledge for security programs and awareness.

The collected data were coded and analyzed by the SPSS for the purpose of extracting needed statistical results. However the Cronbach's alpha reliability coefficient was performed to measure the consistency of the items in the questionnaire (e.g. instrument reliability) and found that, the reliability coefficient was 0.947 and

Table 1. Selected sample size for data collection.

Organization	Total Staff	IT Staff	Non-IT Staff
V	280	14	266
W[*]	96	3	93
X[*]	236	5[**]	231
Y	36	4	32
Z	120	4	116
Population (N)	768	30	738
Sample Size (n) C.L = 95%, C.I = 10.		**23**	**85**

[*] Included the staff at HQ's only. [**] Out of 63 IT staff in HQ and up-countries, only 5 were drawn from HQ running all critical servers.

0.847 for detailed technical questions and general knowledge questions respectively, thus allowing further data analysis and discussions.

5. Results and Discussion

From the data analysis it was found that; 34.7% respondents indicated their organizations had well defined strategies for governing security services and only 18.9% have quantitatively controlled and continuously improving security strategies as shown in **Figure 4**. While only 53.6% respondents indicated their organizations to have well-defined security strategies, questionnaires for non-IT staff demonstrated 41.2% had in-place the information security programs. The distribution of their responses is shown in **Figure 5**. Also, it was noted 32.4% of respondents were not aware of existing information security programs in their organizations. This shows that the selected organizations had limited security training programs or sometimes the formal security awareness programs did not exist at all.

For the purpose of identifying maturity models of the selected organizations, different maturity models (**Table 2**) were used as a benchmark. The average maturity level for all organizations was 2.2 thus concluding that the selected public organizations their security maturity level were in the planning stage and mostly have weak security strategies which require immediate action to protect their IT resources.

Further security analysis was done using the responses from technical detailed questionnaires so as to identify insecurity channels based on STRIDE modelling techniques [16]. For each evaluated security domain, analysis showed that over 69% of responses indicated these organizations to have inadequate security control strategies. The investigated security threats included; spoofing identity, Tempering with data, repudiation, and information disclosure, denial of services and Elevated Privileges. The distribution of their responses is shown in **Figure 6**.

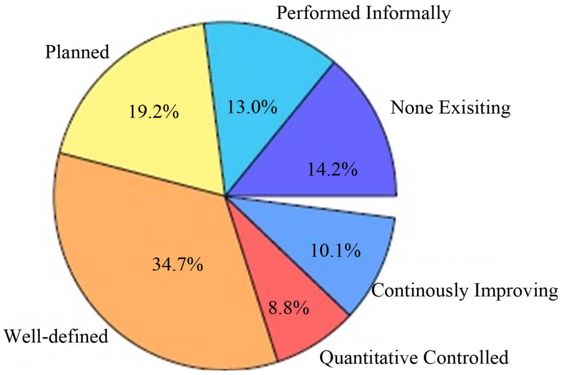


Figure 4. Assessment of Maturity model in selected public organizations.

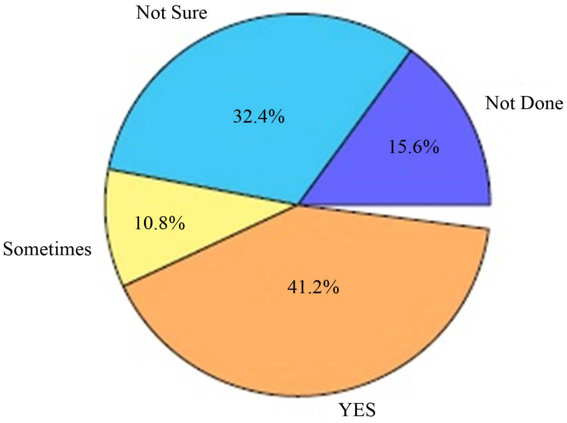


Figure 5. Assessment of general knowledge of information security programs and awareness.

Table 2. Selected sample size for data collection.

Maturity Level	ISO 21827	COBIT	CMMI
0	Not Performed	Non-Existent	Non-Existent
1	Performed Informally	Ad-hoc and Initial	Ad-hoc
2	Planned	Repeatable but Intuitive	Repeatable
3	Well defined	Defined Process	Defined and Implemented
4	Quantitatively Controlled	Managed and Measurable	Managed
5	Continuously Improving	Optimized	Optimized

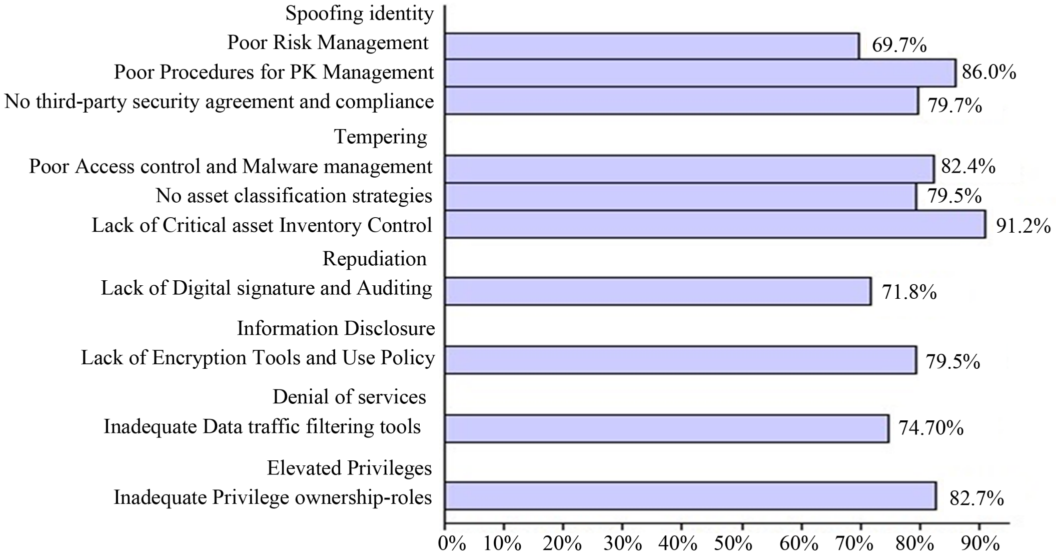


Figure 6. Identified insecurity Channels in selected public organization.

It is the major role for any organization to protect their computer systems, networks, and information from this security attacks such as; unauthorized access, use, disclosure, modification or destruction. Thorough field observations and data analysis, the study has found that this important role was not given high priority in public organizations. However, it was noted that the top management considered the IT security as of less important compared to physical security which is highly considered as critical. For example, after purchase of IT equipments; the set-up for security controls was the business of IT staff. As long as top management find-out the security guards working fine at the gate, then it was assumed that the entire security was good too. Unless otherwise stated, the IT staff was left to figure-out themselves all IT security issues and their controls; from design, configurations and monitoring. Actually, there was no a close eye from top management to oversee whether the security controls implemented by IT staff did comply with organizational security policy or existing best practice. To be specific, the IT experts tried to set-up the security controls based on their security knowledge and sometimes were not able to cover all known and zero-day security holes of a given hardware or system. It is very important the top management to take charge of security management and make sure that the security sense become the part of organization culture. Also, the IT staff should be obliged to put in-place security controls to suite the organization security policy and culture. To ensure well-defined and institutionalized security strategies which suite both organization security policy and culture this study has proposed to:

a) Establish mechanisms for electronic documentation of critical assets and their running services or resources. The study found that about 91.2% had no strategies for managing their ICT assets. It is suggested to automate ICT assets inventory and functions rely on them so that the security experts can strengthen their security controls depending on the classified information (e.g. top secret, secret, confidential or unclassified as major categories in public organizations) stored into these critical assets.

b) Localize the threat assessment tools based on organization's security policy and culture. Despite the little security strategies available in selected organizations, it was noted that no approaches were present for timely assessment and monitoring the compliance of the organization's security policies and existing best practices. It is proposed that the security experts localize or develop appropriate threat assessment tool based on their security policy and culture so that they can be aware of potential threats in each critical assets and thus take appropriate security action.

c) Integrate organization's information security policy into methodologies used for evaluating and documenting organization's critical security threats. It was noted that, no IT risks' register or up-to-date documentation of threats pertaining from organization's critical assets based on their organization risk appetite. It is proposed to automated risk register aligned with the organization's information security policy in order to increase role-based accountability at individual level and organizational structure.

d) Perform timely and appropriate security evaluation to identify security threats from all organization's critical assets. From selected organizations, the study found that only one organization had formal procedures for penetration testing (e.g. ethical hacking) to assess their potential threats or risks. It is suggested to have formal procedure for penetration testing including short-term and long-term strategies for identifying known and unknown vulnerabilities so that the security management can be improved accordingly.

e) Conduct participatory threat-rating for the risk register and documentation. From selected organizations 32.4% respondents indicated not being aware of some basic security controls implemented in their organizations. To ensure effective security controls, the study proposed that all stakeholders should participate in the process of identifying the organization's risks and their controls using top-down approach and vice versa.

f) Escalate appropriately the security threats across organization's operation pyramid. This study found that there exist no formal procedures for communicating security threats or risks across the organization structure. We proposed automated formal communication for any identified threats across organization structure. By doing so, the quick wins can be implemented immediately while looking forward for the long-term strategies.

g) Conduct continuous review and institutionalization. To ensure effective security controls, the continuous review and institutionalization to make security as part of organization culture should be given priority number one in any organization which uses ICT as enabler of her business processes. The study recommended frequently review and institutionalization of security management strategies with back-ups from top management and experts.

h) Conduct continuous awareness and training to ensure information security compliance. The study proposed continuous awareness and training to be conducted frequently using top-down approach and vice versa. For participatory threat-rating and awareness, it's so important to establish information security management unit to oversee the security issues and closer monitoring of information security policy.

6. The Proposed Conceptual Framework

In order to implement the proposed recommendations, the need for automated information security policy mapped with threat assessment tool is proposed. Whether the organization is small or big, it requires information security policy so as to put together the security issues, controls and organization's commitment to protect their critical assets and information stored into these assets. Also, by having the information security policy integrated with threat assessment tools, the organization would have strategic rolling document for benchmarking at any time interval; for example, during the security evaluation processes; any stakeholder in the organization would automatically check and verify the compliance of these security controls without depending on security expertise. To simplify threat assessment processes; this study has proposed the framework (see **Figure 7**) for threat assessment based on the organization's security policy with great focus on organizational environment and culture and also continuous review and institutionalization. The proposed approach evolves in eight phases namely; asset identification, localization of visualization tool, auto-policy integration, auto-threats assessment, participatory threat-register, threat escalation, review and institutionalization and finally awareness and training.

This framework has advantages over other threat assessment frameworks because in the process of assessment it considers:

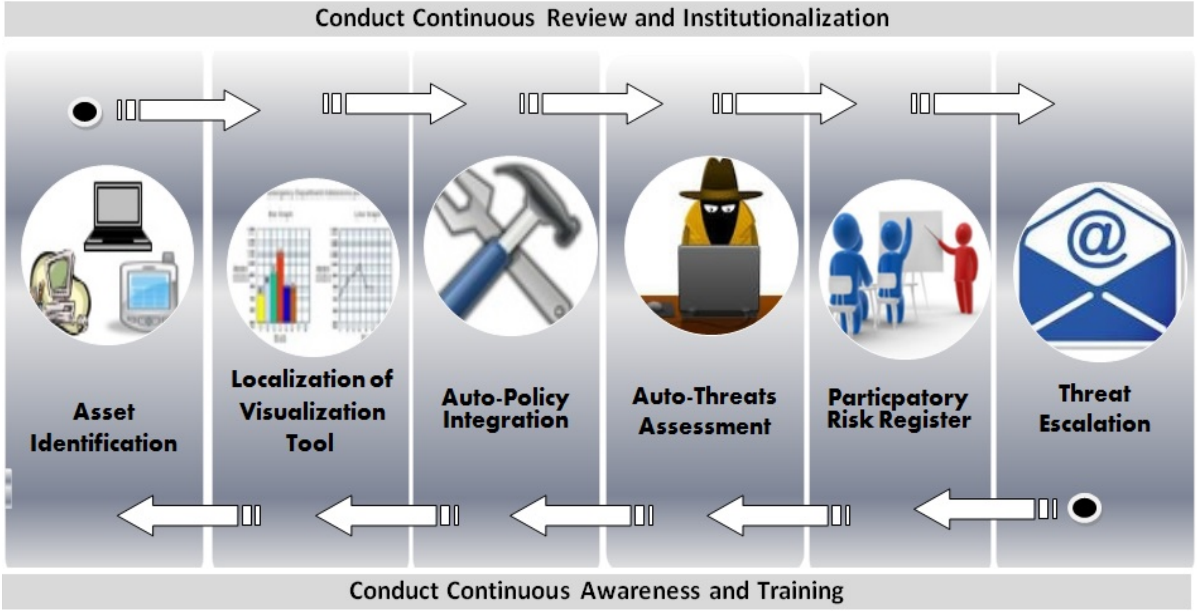

Conduct Continuous Review and Institutionalization
Asset Identification
Localization of Visualization Tool
Auto-Policy Integration
Auto-Threats Assessment
Particpatory Risk Register
Threat Escalation
Conduct Continuous Awareness and Training

Figure 7. Proposed framework for threat assessment based on organization's information security.

- Automation of critical assets inventory and organization's information security policy as artifact of the information security management systems.
- Localization of existing visualization tools based on organization's environment and culture with emphasize on continuous review, institutionalization and participatory risk register and training.
- Forward and backward strategies to ensure continuous threat awareness, monitoring and compliance by using policy automation canvas a proposed tool for requirement engineering during review and institutionalization processes.

As illustrated on **Figure 7**, the goal(s) of each phase is outlined as follows:

- Asset identification phase, the phase proposes to the systems managers to establish an automated inventory control for all ICT assets attached into organization's ICT infrastructures. The establishment of these inventory lists is expected to ensure the closer monitoring of all assets accessing organization's ICT infrastructures such as database servers, mail servers and web servers and thus put appropriate controls to prevent unauthorized asset(s) from accessing the organization's resources without being granted permission.
- Tool localization phase, for effective security management, it's very important to localize the threat assessment tool based on organization's environment and information security policy. It is proposed that, the system developers and security specialists develop or localize appropriately any threat assessment tool based on their security policy and culture. The use of automated information security policy would facilitate the provisions to identify all prohibited asset(s) and resource(s) and thus strengthen the controls for all known vulnerabilities which may be exploited by security threats such as; spoofing, tempering with data, repudiation, and information disclosure, denial of services and elevation of privileges.
- Auto-policy integration phase, the phase propose automatic mapping of security policy and system configuration based on the localized security analysis tool. It's expected that the automatic mapping of the security policy with security analysis tool as a one package, would enhanced the security management and therefore the information security policy become more practical and effective in safeguarding the resources of each asset in the organization.
- Auto-threats assessment phase, this phase prompt automatic penetration testing (*i.e.* ethical hacking) by identifying known vulnerabilities and also search for out-dated applications, services or utilities which can be exploited by attackers to breach the security. After identification of potential threats, immediate communication is done to alert the security managers about these potential threats so as to take necessary action.
- Participatory risk-register phase, after establishment of known and unknown vulnerabilities, this phase propose participatory discussion to identify and document all threats and their associated risks including finan-

cial implications. The goal of this phase is to take on-board all organization's stakeholders in security management. In this case, participatory threat evaluation and rating would establish collaborative IT risk register based on the organization's risk-appetite level.

- Threats escalation phase, after establishment of participatory risk-register, this phase proposes an automated communication tool to communicate these threats across the organization's structure either for notification or immediate action. It's proposed in this phase to put in-place auto-configured elapse time for communicating potential threats across the organization structure.
- Review and institutionalization phase, it's advised to review and institutionalized phases 1 - 6 which serve as the building blocks of the proposed framework. The aim for review and institutionalization processes is to ensure annual strategic rolling plan to mitigate all previous challenges before rolling forward for the next year security planning and management.
- Awareness and training phase, this is the last phase, which prompts the top management to conduct security awareness programs more frequently based on the identified security challenges and threats. It is assumed that for effective security management, every stakeholder should join their hands with IT experts in protecting the organization's critical asset and resources.

For smooth implementation of the proposed framework, we have then proposed policy-automation canvas to translate practically the information security policy into set of quantifiable metrics and therefore evaluate and document automatically the organization's critical threats and their associated mitigation controls and escalation procedures. The key-elements of the proposed policy automation canvas include:

- Strategic Security Control Objective, the unit or individual responsible for information security management system should state clearly the objective of each security control as indicated in the policy.
- Main Security Threat, the stated strategic control objective should be aligned with globally known security threats (e.g. *spoofing identity*, *data tempering*, *repudiation*, *information disclosure*, *denial of services and elevated privileges*) in order to achieve the stated security control objective.
- Identification Key (ID), we propose each main security threat to have identification number for easier follow-up and monitoring of specific threats and their mitigation strategies.
- Specific Threat, state all specific threats associated with main security control by evaluating all security domains using STRIDE threat modelling techniques.
- Insecurity Channels, state all possible security entrance door associated with the stated specific threat by focusing attention on the strategic control objective as a target scope.
- Automation Metrics, state all possible common metrics or check indicators (e.g. attempts and services to check during evaluation process) for quantification during follow-up for compliance and monitoring.
- Standard Mitigation, clearly indicate how to mitigate the specific threats identified with responsible individuals or groups across the organization structure.
- Escalation Procedures, clearly indicate the elapse time for communicating out the specific threat across the organization structure for prompt action to mitigate the threat.

In order to apply the proposed canvas, the organization should identify security issues in all security domains (*i.e.* risk management, access control, communications and operations management, systems development and maintenance, disaster recovery and compliance) and set aside strategic objectives for provision of organization's commitments and mitigation. After stating the strategic control objective, then the STRIDE threat modeling techniques is iterated in all security issues identified and therefore explore specific threats that can be exploited by attacker to compromise the confidentiality, integrity and availability. For each specific threat, checking indicator (e.g. quantifiable metrics) is proposed and thereafter its mitigation and escalation procedures across the organization structure. The example of policy-automation canvas can be illustrated as shown on **Table A1**.

7. Conclusions

Threat modelling has emerged as a viable practice for counter-measuring potential security attacks. Despite the major role of the organization to protect computer systems, networks, and information from these security attacks such as: unauthorized access, use, disclosure, modification or destruction; the study conducted has revealed that this role is not given high priority in public organizations. It was found that about 53.6% of respondents indicated their organizations to have well defined strategies for governing security services and only 18.9% have well-defined and quantitatively controlled security strategies. The lack of effective security strategies at all levels in the organization is expected to promote the exposure of critical resources at the hand of attackers and thus increase the risks and probability of being attacked.

In order to address this problem, we have proposed a conceptual framework (see **Figure 7**) towards threat assessment based on organization's local settings. This framework evolves in eight phases namely; asset identification, localization of visualization tool, auto-policy integration, auto-threats assessment, participatory threat-register, threat escalation, review and institutionalization and finally awareness and training. The proposed framework considers the automation of assets inventory and organization's information security policy as artifact of the information security management systems. An Automated security policy can be through localization of threat visualization tool based on local settings or development of new tool with ability to alert the security managers what are possible threats found in their organizations for quick security mitigation. If this approach is implemented in public organizations, we expect to have an effective evaluation tool which will support security managers to identify potential security threats in their critical assets without depending on security expertise.

Acknowledgements

This research is supported by the Nelson Mandela Institution of Science and Technology under research grant from the Commission for Science and Technology (COSTECH), Tanzania.

References

[1] Fink, D. (1994) A Security Framework for Information Systems Outsourcing. *Information Management & Computer Security*, **2**, 3-8. http://dx.doi.org/10.1108/09685229410068235

[2] Symons, C. (2005) It Governance Framework. *Forrester Best Practices*, **29**, 2005.

[3] Oreku, G.S. and Li, J. (2005) Rethinking e-Commerce Security. *International Conference on Computational Intelligence for Modelling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce*, Vol. 1, 223-228.

[4] Oreku, G.S. and Mbowe, J.E. (2014) Critical Infrastructure Protection. *The International Conference on Digital Security and Forensics* (*DigitalSec*2014), The Society of Digital Information and Wireless Communication.

[5] Yeboah, T. (2013) A Proposed Information Technology Audit Framework for Microfinance Kumasi. *Journal of Engineering Computers & Applied Sciences*, **2**, 1-7.

[6] DBIR (2014) 2014 Data Breach Investigation Report. Verizon Document, Tech. Rep.

[7] Beckers, K., Faßbender, S., Hatebur, D., Heisel, M. and Côté, I. (2013) Common Criteria Compliant Software Development (cc-casd). *Proceedings of the* 28*th Annual ACM Symposium on Applied Computing*, 1298-1304.

[8] Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2003) Introduction to the Octave Approach. Carnegie Mellon University, Pittsburgh.

[9] den Braber, F., Hogganvik, I., Lund, M., Stølen, K. and Vraalsen, F. (2007) Model-Based Security Analysis in Seven Stepsa Guided Tour to the CORAS Method. *BT Technology Journal*, **25**, 101-117. http://dx.doi.org/10.1007/s10550-007-0013-9

[10] Scandariato, R., Wuyts, K. and Joosen, W. (2014) A Descriptive Study of Microsoft Threat Modeling Technique. *Requirements Engineering*, 1-18.

[11] Sommestad, T., Ekstedt, M. and Holm, H. (2013) The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise System Architectures. *Systems Journal*, **7**, 363-373. http://dx.doi.org/10.1109/JSYST.2012.2221853

[12] Keating, C.G. (2014) Validating the Octave Allegro Information Systems Risk Assessment Methodology: A Case Study. Ph.D. Dissertation, Nova Southeastern University.

[13] Abdullah, H. Ooda-Octave, a Novel Approach to Information Security Risk Analysis. http://osprey.unisa.ac.za/TechnicalReports/h5.pdf

[14] Lund, M.S., Solhaug, B. and Stølen, K. (2011) A Guided Tour of the Coras Method. *Model-Driven Risk Analysis*, Springer, 23-43. http://dx.doi.org/10.1007/978-3-642-12323-8_3

[15] ISO 21827 Information Technology Security Techniques. Code of Practice for Information Security Management. http://www.sabs.co.za/content/uploads/files/SANS21827%28colour%29.pdf

[16] De Bruin, T., Freeze, R., Kaulkarni, U. and Rosemann, M. (2005) Understanding the Main Phases of Developing a Maturity Assessment Model.

Appendix

Table A1. Policy automation canvas.

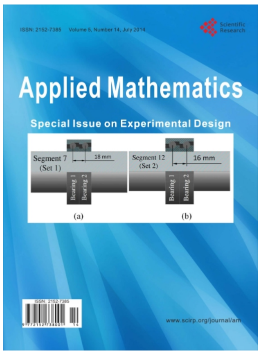
Strategic control objective: *To improve authentication and authorization processes to avoid spoofing identity.*					
Main security threat [STRIDE]: *Spoofing Identity*					
ID	Specific threat	Insecurity channel	Automation metrics	Standard mitigation	Escalation procedures
S001	Camouflage *e-mail to originate from imaginary body*	• *Systems Users* - *Inactive user accounts* - *Unattended computer logins* - *Social-engineering* • Systems Admin, Network Admin and Database Admin - *Inadequate control for removable devices in critical systems* - Poor access rights	• Check frequently - Inactive accounts - *Unsuccessful* password trials - *Password safety and handling*	• Configure appropriately - USB ports - Audit Trail • Appropriate authentication and authorization process • Secure credentials appropriately	**SA»SO»ITM**
S002	Camouflage MAC or IP address to originated from trust source	• Web and Internet - *Inadequate* firewalls - *Poor policy configurations* - Lack of mechanisms for TCP/IP protocols to authenticating the source or destination of message	• Check frequently - The status of ARP log - The status Authentication proxy	Install proxy and packet Filtering Tools	**SA»SO»ITM»CEO**
Strategic control objective: *To prevent data modification, deletion and insertion without appropriate permission.*					
Main security threat [STRIDE]: *Tempering with Data*					
ID	Specific threat	Insecurity channel	Automation metrics	Standard mitigation	Escalation procedures
T001	Back door Malware and Trojans	• Web and Internet - *Inadequate* firewalls - *Poor port configurations*	• Check frequently - Services running - Port scanners	• Appropriate Anti-virus and message authentication process	**SA»SO»ITM»CEO**
T002	Unsecured Data sharing	• Emails and Chatting - *Inadequate mail filters* - *Lack of security awareness*	• Appropriate mail attachments filtering • No of security seminars and workshops	• Digital signature and encryptions • Frequent security training • Prohibit unsecured data sharing	**SA»SO»ITM**

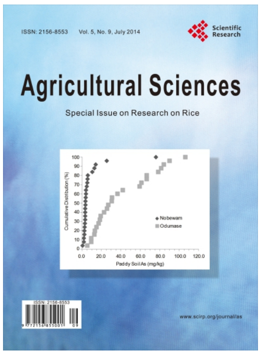
SA—*System Administrator*, **SO**—*Security Officer*, **ITM**—*IT Manager* and **CEO**—*Chief Executive Officer*.

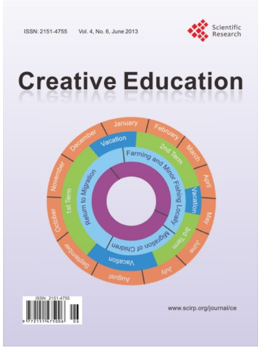
Advances in Bioscience and Biotechnology

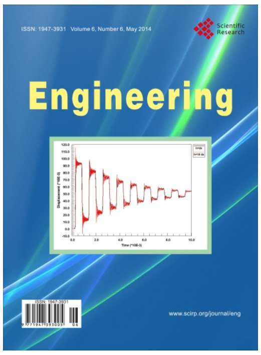
American Journal of Analytical Chemistry

American Journal of Plant Sciences
Special Issue on Photosynthesis

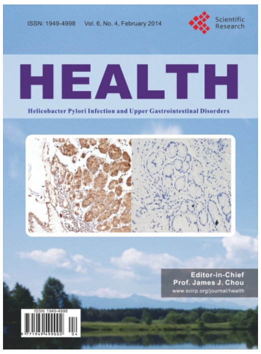

Applied Mathematics
Special Issue on Experimental Design


Agricultural Sciences
Special Issue on Research on Rice


Creative Education

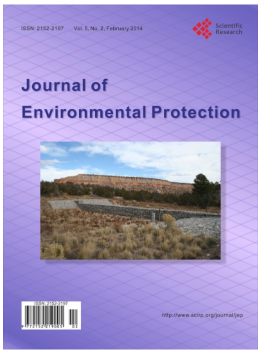

Engineering

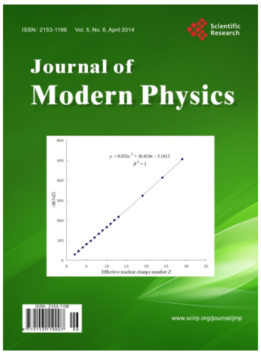
Food and Nutrition Sciences


HEALTH
Helicobacter Pylori Infection and Upper Gastrointestinal Disorders

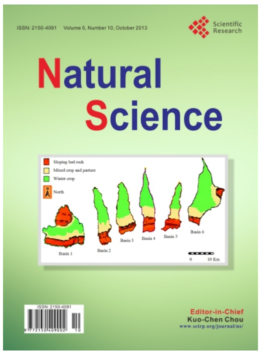
Journal of Computer and Communications

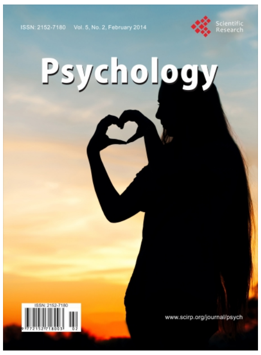
Journal of Cancer Therapy
Special Issue on Bone Tumor Research


Journal of Environmental Protection


Journal of Modern Physics

Modern Economy


Natural Science


Psychology